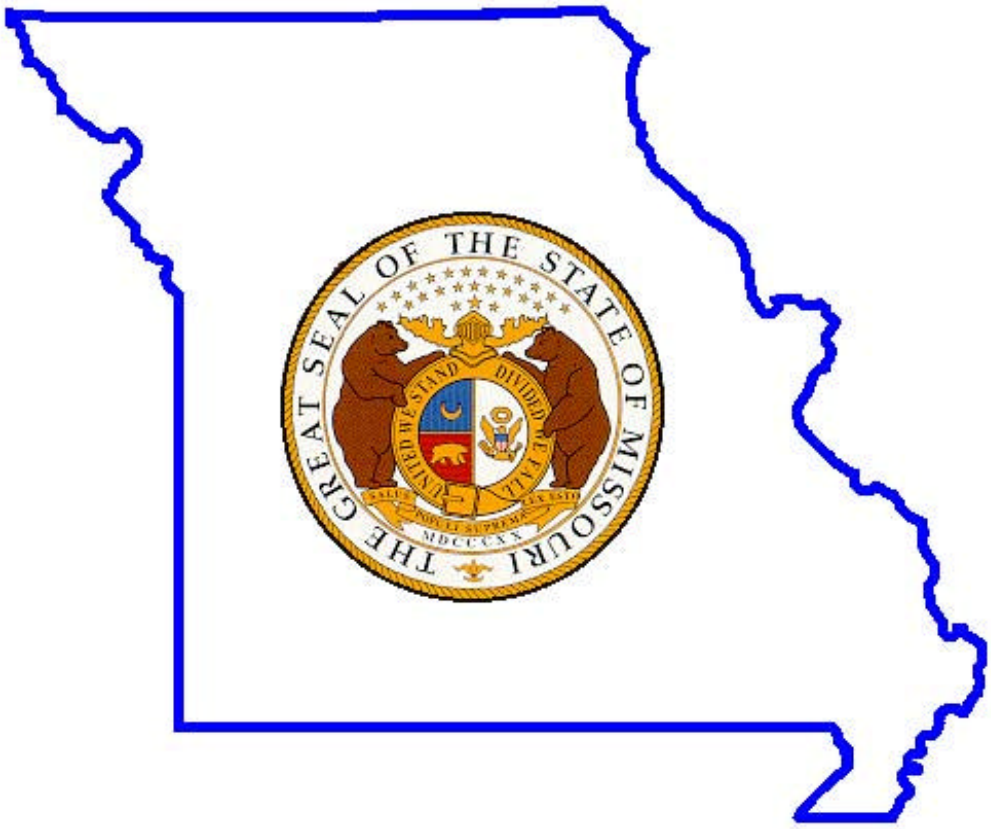
MISSOURI SECURITY PANEL

Utility Committee
Final Report



January 30, 2002

Missouri Security Panel
Utility Committee
Final Report

January 30, 2002

Table of Contents

MISSOURI SECURITY PANEL
UTILITY COMMITTEE
EXECUTIVE SUMMARY

The Missouri Security Panel Utility Committee, comprised of representatives from electric utilities, water utilities, telecommunications companies, natural gas pipelines, natural gas companies, the University of Missouri-Columbia nuclear reactor, the Missouri Department of Natural Resources and the Missouri Public Service Commission, has the charge of evaluating current procedures for safe distribution of utility services and helping various utilities formulate plans which will decrease the likelihood that utility facilities such as a natural gas pipeline, a water system, electric generating plant or a major communications system is subject to a terrorist attack.

The Utility Committee has identified four major goals:

- Identify and assess critical utility related assets for safeguarding management.
- Identify the best practices as they relate to deterring, preventing and responding to a terrorist threat or incident.
- Identify those issues, which might require action by the Missouri General Assembly.
- Identify any type of state, local or federal regulation that might hamper or even prevent the implementation of various recommendations.

A key component of the Committee's work is to receive and evaluate information from those utilities that operate in Missouri. They must clearly and carefully evaluate current business practices; assess risk and vulnerability to their systems; and continue to develop a best practices approach to limit or eliminate the threat of a terrorist attack. Utilities have and will continue to evaluate their facilities that are potential targets.

The Utility Committee has also developed a "best practices" approach for deterring, preventing and responding to terrorist threats or incidents. The "best practices" approach evaluates issues including utility planning, security, enhanced communications and response.

On January 25, 2002, the Missouri Security Panel presented its top five recommendations to the Governor and Tim Daniel at a meeting held at Washington University in St. Louis. Along with the top five Utility Committee recommendations, each utility subcommittee had additional recommendations to enhance and improve security of utility infrastructure. Some of these recommendations have been implemented or are in the process of implementation. Some of the utility recommendations may take several years to implement which is why it is critical that issues of security stay at the forefront of the utilities and both state and federal government.

Missouri Security Panel
Utility Committee
Top Five
Findings and Recommendations

Presented to the Missouri Security Panel
January 25, 2002

Outline

- **General Findings & Recommendations**

- **Best Practices**

- **Specific Findings & Recommendations**

General Finding & Recommendation

Finding: By their very design, utility systems are vulnerable to terrorist attack. However, the specific points of vulnerability are difficult to determine. Identifying the critical assets of utility systems is equivalent to identifying these points of vulnerability. There is a need to protect this information because knowledge of these vulnerable points and critical assets could provide a "roadmap for terrorists."

Recommendation: We recommend that the critical assets of utility systems should not be identified in the Key Asset Protection Plan or any other report prepared by the Missouri Security Panel. We also recommend that each utility in Missouri develop its own internal list of critical assets and security guidelines. We also recommend that a contact person at each utility in Missouri be identified to coordinate with state and local officials if a specific threat is made.

Best Practices Finding & Recommendation

On October 31, 2001, the PSC Staff surveyed all Missouri utilities to develop a Best Practices list for utility emergency preparedness (Case No. OO-2002-202).

Finding: Missouri utility companies who responded to the survey indicated preparedness for a variety of types of emergencies.

Recommendation: All Missouri utilities should be encouraged to review the Best Practices list and, where applicable, adopt those items they are not currently performing.

"Best Practices"
for
Improving Security

- Keep employees informed and promote a state of higher vigilance
- Require employees and visitors to wear IDs on company property
- Increase patrols and log security status by employees at company offices
- Monitor requests for system information from outside sources-Require that all information requests be in writing on company letterhead and only give out information with management approval
- Conduct communication checks on a periodic basis and provide additional communication devices; i.e., radios, cell phones, etc., for employees
- Encourage employees to be aware of their surroundings while working on system facilities
- Increase patrols and log security status of employees around the system
- Encourage employees to take all system alarms, routine or otherwise, seriously and investigate the alarms to verify system status
- Meet with local, state, federal, and possibly military law enforcement to increase awareness and to assist in patrolling key facilities and responding to emergencies
- Develop threat response levels to ensure response is appropriate to threat
- Develop security and staffing procedures relative to each of the threat levels
- Install new or additional protective barriers to manage and protect access to aboveground facilities as needed
- Add third-party security forces if needed
- Add additional electronic surveillance equipment such as cameras, motion alarms, etc., as needed
- Increase use of SCADA systems to monitor system operating conditions at critical facilities
- Change locks on all facilities to better manage access—review possible use of programmable and other high security locking devices
- Lock all valves (critical or non-critical) at aboveground facilities
- Secure all company equipment (valve keys, etc.) vehicle supplies, and vehicles when not in use
- Inventory company critical tools and equipment and manage more closely to prevent theft and use by unauthorized persons
- Limit access to excavations around facilities and do not leave the excavation open for extended periods of time
- Monitor excavation activities around critical facilities
- Conduct table top exercises, field exercises, mock disaster drills
- Have adequate tools, and equipment in inventory to repair or replace critical and/or site specific emergency response equipment
- Establish alternate communication systems in event of primary communication system failure
- Review alternate access routes to critical infrastructure in case primary route is unavailable
- Stage equipment to allow quick response—example, what if tunnels or bridges are not accessible?
- Determine what "out of the ordinary" equipment may be necessary to ensure access
- Meet with contractors in your area to evaluate what equipment they may have for use in the event of emergency
- Provide for alternate power supplies and periodically test them to ensure operation
- Have adequate vehicle and equipment logistics available-fuel, tires, spares, etc.
- Frequently meet with local law enforcement officials and health officials to discuss preparedness plans

Specific Finding & Recommendation

#1 - Electric

Finding: Security at the Callaway Nuclear Plant is adequate. As a result of September 11, 2001, the Nuclear Regulatory Commission (NRC) is expected to develop additional security requirements for nuclear power plants.

Recommendation: We recommend continuing to comply with all requirements set by the NRC and Congress.

Specific Finding & Recommendation

#2 - Water

Finding: Some utilities in Missouri do not currently carry a disinfectant residual throughout their water distribution systems. This leaves the system with little or no defense against contamination, either accidental or intentional.

Recommendation: We recommend that all water utilities serving 10,000 or more people be required to maintain a disinfectant residual throughout the distribution system as a means to reduce risk during a terrorist attack.

Specific Finding & Recommendation

#3 - Electric

Finding: An explosion of sufficient magnitude could breach dams at hydroelectric power plants.

Recommendation: We recommend that a feasibility study be conducted to determine if truck, van, and/or other traffic across dams should be restricted.

Specific Finding & Recommendation

#4 - Pipelines and Gas

Finding: Only one bridge in Missouri has a gas line attached to it. Most river crossings are independent suspensions or buried lines.

Recommendation: We recommend that operators should perform vulnerability assessments and be cognizant of unusual situations while patrolling lines.

This Pipeline Recommendation should also be included as part of the Transportation Committee's final report.

Specific Finding & Recommendation

#5 - Telecommunications

Finding: In the event a major emergency situation occurs, an expedited process for communication among companies and agencies would be useful.

Recommendation: We recommend that the companies should work with representatives of law enforcement and emergency agencies to coordinate a single point of contact for major emergency situations recognizing that this contact is not designated for routine responses.

APPENDIX

Water Subcommittee

Overview

Recent terrorist activities have heightened concern about potential, deliberate attacks on public water supply systems. In the State of Missouri, there are over 1440 water providers serving 4.7 million people, or 84% of the 5.6 million citizens. Incredibly, over 1,420 of these utilities serve 10,000 customers or less. This fact alone points up both the relative strength and weakness of the state's water utility network as it pertains to its ability to respond to a terrorist threat or attack.

The highly fragmented nature of the water utility infrastructure in Missouri does provide a natural defense against a massive scale terrorist attack, given the dispersed assets and sources of supply. However, it also significantly complicates our ability to achieve standard levels of threat response, redundancy, and communication.

The largest single water systems in the state serve St. Louis County, Kansas City, and St. Louis City respectively. Each of these organizations has taken dramatic steps to protect their critical infrastructure. Additionally, major cities such as St. Joseph, Joplin, and Jefferson City have taken similar measures. The largest three systems also provide the water supply to an additional 34 secondary systems. Throughout the state, there are a total of 300 secondary systems.

The smaller water utilities across the state typically struggle with financial and technical support. However, there is an abundance of best practice information available through industry sources such as the American Water Works Association that can assist these smaller entities in evaluating reasonable risks and vulnerabilities. It seems unlikely that a terrorist attack would occur on some of the smaller utilities because of the lack of dramatic impact. While it is advisable for these systems to undertake prudent measures to limit access to critical facilities and train all responders, further extensive measures would appear unnecessary.

Planning Approaches

The perpetrators of manmade security risk include employees, vandals, disaffected groups within the community, domestic extremists or foreign-based terrorist organizations. No single set of hazards or threats are appropriate for all utilities. What is generally accepted is that protecting water supply systems and critical infrastructure components is essential. Providing reasonable security for these systems no longer can be taken for granted and viewed as normal operating protocols. Understanding risk analysis and response to today's security threats is essential and requires utilizing professional evaluations and consistent best practices. While security assessment, response plans, and security systems are critically important and valuable, the effectiveness of these tools is dependent on the skills and diligence of the staff applying the tools. First and foremost a comprehensive review of all the necessary elements for a utility to produce safe and sufficient water must be evaluated for vulnerability or disruption.

Effective Security efforts are clearly the result of a Strategic Planning Methodology. There are no Federal security standards for water utilities, so that each system must use available expertise, common sense and commitment. As facility design and construction events occur, or as existing systems are evaluated, security measures should now be integral to the process. Risk assessment and Target inventories should also be developed for each water system. This information must be carefully guarded and protected. For many of the states smaller utilities, this can still be very simple and cost effective to do. For more advanced reviews, there are analytical tools available to assist in evaluating the relative risks and rewards of such efforts.

In a report to the US Congress titled **Combating Terrorism-Threat and Risk Assessments Can Help prioritize and Target Program Investments** (GAO/NSIAD-98-74), a simple yet effective decision-making model is reported. It uses a formula approach where

$$C = .5F = .3U = .2E$$

C represents the relative Consequences
F is the relative adverse health effects
U is the facility down time resulting from the attack
E is the Exposure to Public outcry or dismay

(Ratings of 0-5 are applied, with 0 being very low and 5 very high)

The higher the consequences, then clearly the higher the target value. The attractiveness of the target then comes into play. A utility serving a vacation destination or National Monument would of course increase its attractiveness as an example.

There are other similar techniques like this available for water utilities to employ. However, simply stated, water treatment plants, sources of supply and tanks are clearly critical and should be protected.

General Security Considerations

There are many modest steps that can be taken to improve security overall. A simple yet effective approach is to build the system along three strategies;

- deny access,
- detect incursions, and
- respond rapidly.

Site and perimeter security is the first stage of importance. Buildings, and critical assets on site such as wells, tanks, basins, and treatment plants are next. Simple systems such as fencing, lighting, intrusion alarms, secured doors and windows all should be evaluated and deployed as needed. Employee safety is also critical. Systems such as Identification Badges, background screening, and proper control of keys etc. are basic, yet crucial. Visitor sign in and restricted parking areas should be in place as well. Video surveillance is also quite cost effective today and should be widely considered.

Monitoring for turbidity, chlorine residual, and pH can be excellent indicators of system integrity and tools for the early detection of introduced agents and subsequent response. Integrating this monitoring equipment with alarms and alert systems should be done with remote facilities such as tanks and critical boosters. For large, critical water treatment facilities serving major population and government centers, 24-hour security by trained professionals should now be the norm.

Finding

It should be noted that some utilities in Missouri do not currently carry a disinfectant residual throughout their water distribution systems. This leaves the system with little or no defense against contamination, either accidental or intentional.

Recommendation

Require that all water utilities serving 10,000 or more people maintain a disinfectant residual throughout the distribution system as a means to reduce risk during a terrorist event.

Redundancy in terms of energy and supply are very important. Back-up generators and adequate storage and supply capacity should be evaluated. Electric utilities have required reserves, but no such mandatory guideline exists for water systems. While it can be difficult to develop a simplistic formula, due to the nuances of water systems such as storage and interconnections, a more robust system of guidance would be beneficial.

Finding

The large number of water utilities in the state, combined with the lack of federal or state guidelines for redundancy, suggests some vulnerability to supply interruptions.

Recommendation

Encourage the interconnection of water utility's distribution system so that emergency supplies are readily available.

Finding

Even though additional security measures are required and prudent, the funding for such endeavors can be quite difficult for many utilities. Obstacles can result in a disincentive for action.

Recommendation

Remove impediments to all utilities so that the cost of additional security is rapidly reflected in the rates they charge, consistent with prudent implementation.

Communication

In times of crisis, effective communications can make all the difference. Water utilities should have an updated Emergency Response Plan, which would now include Terrorist Attacks as a scenario. An updated call list for all major governmental agencies and resources that could be needed during an event should be included. State and local Emergency Response Task Forces should be an integral part of the utilities response system. Coordination and training, utilizing mock disasters and tabletop exercises, should be done annually. With each training session, lines of communication will be enhanced and problems identified for resolution. It should be noted that the Missouri Security Panel Resource Guide CD is an excellent resource that should be distributed to all utilities.
Equipment for communicating is important as well. Redundant systems, such as landlines and cellular facilities should be available within all water utilities. Additionally, the use of new broadband systems currently under development could ultimately be deployed as well.

Communicating with the public is also vital. While it would be imprudent to broadcast the measures taken by each utility, the public's assistance should be sought. Often times, citizens live and work around facilities such as wells, tanks, hydrants, and water treatment facilities. The public can be encouraged to report suspicious activity, and know how to identify threats from everyday activities.

Findings

Many water utilities typically did not include Terrorist attacks as a scenario in their Emergency Operations Plans. Additionally, because of the large number of municipally owned utilities present in this industry, there is no ability to maintain the confidentiality of the plan.

Recommendations

Require all utilities to include in their Emergency Response Plan (EOP) contingencies for terrorist attack.

Encourage major utilities to annually conduct attack response drills to facilitate effective communication and activity coordination with local first responders.

Enact legislation that would allow portions of the EOP to remain confidential, even to Freedom of Information Act requests.

Gas Subcommittee

Terrorism Threat Awareness:
We found that most natural gas operators have a general understanding and awareness of issues related to terrorism. The depth of knowledge of specific topics such as advanced security measures, Potential Threat Elements (PTE's), the types of terrorism and Weapons of Mass Destruction (WMD), however, varies from operator to operator.

We recommend that a summary document on specific topics related to preparation for, response to and recovery from acts of terrorism be identified or developed and that natural gas operators be made aware of how to acquire the document.

Risk Assessment:
We determined that most natural gas operators had performed some type of vulnerability assessment on their facilities. In some cases the review had been prompted by the Missouri Public Service Commission (MPSC) Staff, which had prepared and had asked each jurisdictional utility to complete and submit a security survey form. The survey addressed issues related to preparedness for and response to acts or threats of terrorism. The survey did not attempt to address the degree of impact of a terrorism incident.

We recommended that natural gas operators perform a vulnerability self-assessment for their assets and to provide the results in summary form. The results could be used to help identify operators who have facilities that should be included in the State's safeguarding management plan.

To help ensure some degree of consistency in the evaluations among the operators, a vulnerability assessment form was developed. The form allowed the operators to evaluate their facilities on a numerical rating basis in terms of visibility, target value to potential terrorists, criticality, site population, potential for collateral damage, potential for mass casualties, ease of access and hazardous materials at the facility. The operators were asked to provide the cumulative vulnerability assessment numerical rating for their top three rated facilities. Of the approximately 90 operators contacted, vulnerability assessment results were received from 13 companies including the major natural gas operators in the state. Of the companies that responded, 8 may have a facility that has a rating that might warrant additional consideration, evaluation and review by the National Guard for inclusion in the State's safeguarding management plan.

We recommend that the natural gas operators be encouraged to review key facilities to determine if vehicle barriers might be helpful in making such facilities less vulnerable to terrorist attacks and to review their storage procedures for chemicals such as odorant to determine if additional security measures should be taken to ensure that such chemicals are not improperly used by terrorists.

Detection and Deterrence:
We found that the natural gas operators consider their security to be generally adequate. Many do, however, realize that some enhancements may warrant consideration. The security measures typically employed by natural gas operators are not intended to make facilities defendable from determined attackers, but are intended to deter and detect an attack and facilitate properly responding to an attack or a threat of attack.

We recommend that the natural gas operators be requested to consider specific additional security measures for applicability to their facilities. Such additional security measures would include, but not be limited to, additional camera surveillance, more restrictive facility access procedures, hardening of facilities (e.g., installation of barriers, guard rails, etc.), public parking restrictions, and increased efforts to secure vehicles when not in use. Gas industry organizations such as the American Gas Association (AGA) and the Interstate Natural Gas Association of America (INGAA) are working with the Federal Office of Pipeline Safety (OPS) to develop additional guidelines and regulations for maintaining an adequate level of security for gas facilities. **We recommend that consideration be given to using the Missouri Association of Natural Gas Operators (MANGO), whose membership includes representatives from the natural gas operators and the MPSC Gas Safety Staff (Staff), as**

the conduit through which information could be disseminated and discussed among the State's operators and the Staff.

Gas Operator Action Plans:

We found that the most natural gas operators have plans for responding to different types of facility problems and natural disasters. These plans are, however, typically reactive in their approach. The plans describe how to react to particular types of events.

We recommend that the natural gas operators develop an addendum to their plan that would document how to respond to different levels of terrorism threats and to different types of terrorism incidents. This addendum could be used to document the results of the facility vulnerability self-assessment and the temporary actions to be taken to increase security based on the level of terrorism threat that exists. A key part of this addendum would be the description of the threat condition states, a listing of events that would initiate a response by the operator and what that response would be. These temporary actions would typically not involve any permanent changes to an operator's facilities. Gas industry organizations such as the American Gas Association (AGA) and the Interstate Natural Gas Association of America (INGAA) are working with the Federal Office of Pipeline Safety (OPS) to develop a general description of four different Threat Condition States: normal, low, medium and high. **We recommend that consideration be given to using the Missouri Association of Natural Gas Operators (MANGO), whose membership includes representatives from the natural gas operators and the MPSC Gas Safety Staff (Staff), as the conduit through which information for use in developing action plans triggered by different Treat Conditions States could be disseminated and discussed among the State's operators and the Staff.**

Response to an Act of Terrorism:

We found that most natural gas operators have already developed an emergency response plan that is applicable to responding to acts of terrorism. The plans are typically intended to deal with specific types of events that could occur at various types of facilities. The plans include provisions for protecting life, both the public and employees, and property. The plans also include procedures for communicating with local emergency responders. Most operators maintain an active liaison with local emergency responders. The plans are reviewed and updated annually. Operator personnel are trained on the procedures. Many operators also developed plans to deal with more wide spread events such as floods, earthquakes, loss of communication and major system outages.

We recommend that operators be encouraged to develop additions to their plans that would address how to respond to an act of terrorism on a facility-specific basis, on a local basis and on a regional basis. These additions would include communication protocols, joint response actions, supporting law enforcement investigations and the roles to be played by the operator and government. Gas industry organizations such as the American Gas Association (AGA) and the Interstate Natural Gas Association of America (INGAA) are working with the Federal Office of Pipeline Safety (OPS) to develop additional guidelines for responding to terrorism events. **We recommend that consideration be given to using the Missouri Association of Natural Gas Operators (MANGO), whose membership includes representatives from the natural gas operators and the MPSC Gas Safety Staff (Staff), as the conduit through which information could be disseminated and discussed among the State's operators and the Staff.**

Telecommunications Subcommittee

Findings

- Industry and Government Security initiatives are currently conducted at the Federal Level and do not need to be duplicated at the state level.
- Current industry standards include provisions for network survivability, redundancy, and recovery.
- Most telecommunications companies have disaster recovery plans and procedures in place.
- In the event a major emergency situation occurs, an expedited process for communication among companies and agencies would be useful.
- The network, by its very nature, is susceptible to tampering buy outside parties.

Recommendations

- **Ensure that local law enforcement agencies coordinate with federal law enforcement agencies in the event specific threats are received.**
- **Advise carriers of the need to adhere to current industry standards for network survivability, redundancy, and recovery.**
- **Advise carriers to review disaster recovery plans and procedures and, if necessary, update those plans.**
- **The companies should work with representatives of law enforcement and emergency agencies to coordinate a single point of contact for major emergency situations recognizing that this contact is not designated for routine responses.**
- **The penalties for tampering with the network could be increased from a misdemeanor to a felony under certain specified guidelines.**

Identification of Critical Assets

- **Carriers do not want to identify specific critical assets because of security and competitive reasons. In general, critical assets would include end-office switches, tandem switches, and transmission facilities and customer care call centers.**

Electric Subcommittee

The findings and recommendations for the electric sector are:

- Security at the Callaway Nuclear Plant is adequate. As a result of September 11, 2001, the Nuclear Regulatory Commission (NRC) is expected to develop additional security requirements for nuclear power plants. **We recommend continuing to comply with all requirements set by the NRC and Congress.**

- By its very design, the electric system is vulnerable to terrorist attack. However, the specific points of vulnerability are difficult to determine. Identifying the critical assets of the electric sector is equivalent to identifying these points of vulnerability. There is a need to protect this information because knowledge of these vulnerable points and critical assets could provide a "roadmap for terrorists." **We recommend that the critical assets of the electric sector should not be identified in the Key Asset Protection Plan or any other report prepared by the Missouri Security Panel. We also recommend that each electric utility in Missouri develop its own internal list of critical assets and security guidelines. We also recommend that a contact person at each electric utility in Missouri be identified to coordinate with state and local officials if a specific threat is made.**

- An explosion of sufficient magnitude could breach dams at hydroelectric power plants. **We recommend that a feasibility study be conducted to determine if truck, van, and/or other traffic across dams should be restricted.**

- FERC has concluded that $12.6 billion is needed to fix major bottlenecks in the nation's transmission system. A September 20, 2001 report titled *National Security and State Public Utility Commissions* concluded that, "Increased security may require redundant utility facilities." **We recommend increased investment in critical energy infrastructure to provide additional redundancy in the electric system.**

Pipeline Subcommittee

Finding

Only one bridge in Missouri has a gas line attached to it. Most river crossings are independent suspensions or buried lines.

Recommendation

Operators should perform vulnerability assessments and be cognizant of unusual situations while patrolling lines.